GLOBUS

Cosmos An International Journal of Management
A Refereed Research Journal
Vol 11 / No 1 / Jul-Dec 2021 ISSN: 2278-1218

ACTS RELATED TO BANKING SECTOR CONSIDERING TECHNOLOGY AND CYBERCRIME

*Rakesh Singh
**Dr Atal Kumar

Paper Received: 06.11.2021 / **Paper Accepted**: 04.12.2021 / **Paper Published**: 05.12.2021
Corresponding Author: Rakesh Singh; Email: rakesh745892@gmail.com; doi:10.46360/cosmos.mgt.420212019

Abstract

Cybercrimes have increased as a result of the advent of an age in technology for banking that has removed the requirement for physical presence with the bank for numerous transactions and other financial services by using electronic devices. E-banking has made a significant and noteworthy contribution to this boom, given that consumers are increasingly reliant on the internet for everything from small-scale financial transactions to complex financial matters. This study discusses about various acts related to banking sector considering technology.

Keywords: Cybercrime, Banking Sector, Technology, Act, Punishment.

Introduction

A method of communication & information storage on paper that makes it easier to send documents electronically to government organisations. The Reserve Bank of India Act of 1934, the Indian Criminal Code of 1860, the Indian Proof Act of 1872, and the Banking Certificates Act of 1891 were also altered by the IT Act. The Act aims to achieve the following goals:

1) legal recognition of all transactions made by means of electronic data exchange or other electronic means of communication or electronic commerce, instead of the earlier paper communication method;
2) legal acknowledgement of digital signatures to authenticate any information or matters requiring legal autentification;
3) facilitation of the electronic submission of documents to government bodies as well as to departments;
4) facilitating the electronic storage of data;
5) establishment of legal sanctions and facilitation to the electronic transfer of funds between banks and financial institutions;
6) legal recognization of the legality of electronic bookkeeping in accordance with the Evidence Act of 1891 and the Reserve Bank of India Act of 1934.

Review of Literature

Acharya, and others (2020) [1] The impact of cyberattacks on banking institutions was examined in the research paper that followed by using actual bank attack cases, such as the 2017 attack on UBI, which was carried out through phishing through an email, and the malicious strike on Cosmos Bank in Pune, which was carried out through malware attack, disrupting the bank's services. ATM services were affected, and the number of cyberattacks involving nationalised banks and private sector banks was compared to determine the effect on the financial industry.

In 2019, Harshita [3]; The research paper discussed the prevalence of cybercrimes within the banking industry and the data and cases that were presented. The banking industry was targeted in cases involving emails, mobile banking, and internet banking, which are all initially vulnerable and easily targeted by cybercriminals. and talked about how the increase in cell phones with online access has had a severe influence on the incidents of cybercrimes that have been uncovered. These days, cell phones are used for many internet activities such as online shopping, online money saving, online service fee payment, and, according to the offenders, continuous access to personal information.

2020's Sarangam [4]; The difficulties with cyber security were discussed in the article below. Ajay Saragam highlighted a number of issues in India, including the absence of a national cybersecurity infrastructure, Absence of division Since there are no borders in cyberspace, unlike in nations or governments, this leaves the armed forces, ONGC's digital assets, banking operations, and other institutions open to cyberattacks from anyplace. Due to the lack of a cybersecurity regulatory authority, this could lead to national security breaches that cause loss of money, property, or lives. In the upcoming days, these kinds of obstacles must be overcome in order to build cybersecurity at the federal level.

*Research Scholar, Himalayan Garhwal University, Shiv Nagar, Phokra, India.
**Research Supervisor, Himalayan Garhwal University, Shiv Nagar, Phokra, India.

Analysis

The Reserve Bank of India is the primary regulator of banking in India. "RBI has broad powers to govern the financial sector, including corporate governance and organisation, prudential regulations and limitations for product and service structuring, payment and settlement system oversight, currency management, and the establishment and licencing of banks, including foreign bank branch offices in India."

The Reserve Bank of India has made it clear time and time again that both general norms and specific regulations are used to regulate digital banking legally (2019, RBI). The following general rules apply to banking in India:

1) the Banking Act 1949;
2) the Foreign Currency Management Act 1999;
3) the Reserve Bank of India Act, 1934;
4) the Payment and Settlement Systems Act, 2007;
5) the Payments and Settlements Systems Regulations of 2008 and the BPSS Regulations, 2008; and
6) the Amendment of the payment and settlement systems Act of 2015.

Furthermore, some general regulations have been published by the Reserve Bank of India:

1) Real-Time Gross Settlements System Rules (RTGS) 2013;
2) Rules for Applying for Authorization from Foreign Principals for Transboundary Money Transfer Services to India;
3) Interbank Settlement Rules;
4) Procedural Guidelines for the Checks System.

1. Specialized Acts

The Committee for Internet Banking was formed by the Reserve Bank of India to look into many facets of online banking. The three primary areas of Internet banking that the Committee addressed were technological and security challenges, legal issues, and regulatory along with supervisory issues. Following the Working Committee's adoption of its suggestions and recommendations, the RBI released Instructions: Internet Banking in India 2001. "Only those banks that are licenced as well as supervised in India with a physical presence within India will be permitted to provide online banking services to residents of India," that is to say, "only those banks that are registered outside the nation and are not physically present in India, including traditional banks as well as virtual banks, are allowed to provide internet banking products and services to Indian residents." The guidelines also mandated that banks use a reveal template to compel clients to disclose the risks, liabilities, and responsibilities associated with doing business over the Internet. Banks were also forced to disclose their most recent financial data that have been published online.

The Reserve Bank established the Electronic Clearing Service Scheme (ECS) Credit in the 1990s to handle large-scale, periodic payment claims (including dividend, interest, and labour payments). The technology is currently accessible in all of India's main cities and makes it simple for clients to deposit money into their accounts on a designated day. At the National Clearing Unit, in Mumbai, the Reserve Bank introduced a new service in September 2008 called the National Electronic Clearing Service (NECS). For every debit to the sponsor bank account, NECS allows for numerous debits to recipient accounts at various branches across the nation. Utilising the Core Banking Solutions (CBS) of the participating banks, the system is available throughout India and makes it possible for all CBS subsidiaries, no matter where they are located in the nation, to participate. When the Electronic Funds Transfer (EFT) system was implemented in the late 1990s, owners of bank accounts could electronically transfer money to other owners of bank accounts at any other bank that was a participating bank.

The National Electronic Funds Transfer System (NEFT), a multipurpose system, took the place of this one in 2005. 2004 saw the introduction of the Real-time Gross Settlements System (RTGS). Money can be exchanged between banks using the Real-Time Gross Settlement (RTGS) system in both real-time and gross terms. When a payment transaction is settled in real-time, there is no waiting period.

A transaction is considered to be in "gross settlement" if it is computed individually without being combined or compensated with another transaction. Payments are finalised and non-refundable after processing. In April 2001, the Clearing Corporation of India Limited (CCIL) was founded. Primary dealers, banks, and financial institutions were involved in the formation of CCIL. For the purpose of clearing and settling transactions within the money marketplace, government securities, and foreign currency markets, CCIL functions as an industry support & services organisation.

Prepaid Payment Systems are a system about prepaid payment instruments developed by the Reserve Bank of India. Payment instruments that permit the purchase of goods and services at the expense of the value stored on them are known as prepaid instruments. Examples of these include smart cards, magnetic tape cards, Internet accounts, Internet wallets, mobile bills, and mobile wallets.

The value that is held on these instruments is the amount that the holders have paid using cash, a credit card charge, or a bank account debit. The Reserve Bank of India released Guidelines for the issuing and management of prepaid instruments in India based on the Payment & Settlement Systems Act of 2007. The policies went into effect on December 12, 2018. Prepaid payment instruments are only allowed to be used for cross-border transactions if they are authorised under the Foreign Exchange Management Act of 1999.

A collection of operating guides for mobile banking was released by the Reserve Bank of India in 2008. A Master Circular (Master Circular) outlining the prerequisites for mobile banking offered by Indian banks was released later in 2016. This circular states that the only banks that can provide mobile banking via the Reserve Bank's approved systems are those that hold an RBI licence and have a physical location in India.

The Circular addressed authorised RBI systems (RBI) for interbank transfers and security systems. The Reserve Bank has been granted permission by the National Payment Corporation of India (NPCI) to enhance the quantity of mobile banking services and broaden the reach of IMPS (Immediate Payment Service) channels, encompassing ATMs, mobile devices, and the Internet. In parallel, NPCI is attempting to expand the number of mobile service providers that have access to a single platform for mobile banking services.

In order to encourage and assist emerging financial technology, or FinTech, the Reserve Bank of India including its Specialised Committee for Internet Banking have undertaken a variety of projects and activities.

1) permitted non-banking entities to operate payment systems and offer technical services in the payment field.;
2) BBPS (Bharat Bill Payments System) was put into place, enabling non-cash payments.;

3) released the Consultative Document concerning Card Infrastructure, a Consultative Paper about Card Payment Infrastructure;

4) held a consultation regarding peer-to-peer, or P2P, lending;

5) released the Guidelines for Account Aggregators (Instructions on Aggregators).

6); were created by digital payment schemes using the guidelines of the Inter-User Approval of Corporate Payments and the National Payment Facility. These also allow for the collection of electronic payments to be charged based on digital bills and made available to the national bank under the guidelines of IPPIIP, which serves as a joint payment address for corporate payments approvals and the National Payment Facility.

2. Punishments, Compensation & Adjudication

Sec.43: If any individual without authorization of the proprietor harms to PC, PC framework, and so forth he/she will be obligated to pay remuneration to the individual so influenced.

Sec.43A: Where a body corporate, having, managing or taking care of any delicate individual information or data in a PC asset which it possesses, controls or works, in careless in executing and keeping up sensible security practices and strategies and along these lines makes unfair misfortune or improper addition any individual, such body corporate will be subject to pay harms by method for remuneration to the individual so influenced.

Sec.45: Whoever repudiates any standards or guidelines made under this Act, for the negation of which no punishment has been independently given, will be subject to pay a remuneration not surpassing twenty-5,000 rupees to the individual influenced by such contradiction or a punishment not surpassing twenty-5,000 rupees.

Sec.66: If any individual, deceptively or falsely, does any demonstration alluded to in segment 43, he will be culpable with detainment for a term which may reach out to three years or with fine which may stretch out to five lakh rupees or with both.

Sec.66B - Punishment for unscrupulously: Accepting stolen PC asset or specialized gadget is Imprisonment for a term which may stretch out to three years or with fine which may reach out to rupees one lakh or with both.

Sec.66C - Punishment for data fraud: Whoever, falsely utilize electronic mark or secret phrase, will be at risk for detainment for a term which may stretch out to three years and will likewise be at risk to fine which may reach out to rupees one lakh.

Sec.66E - Punishment for infringement of protection Whosoever, purposefully or intentionally catches, distributes or transmits the picture of a private zone of any individual without his or her assent, under conditions abusing the security of that individual, will be rebuffed with detainment which may reach out to three years or with fine not surpassing two lakh rupees, or with both.

Sec.66F - Cyber fear mongering Imprisonment which may reach out to detainment forever.

Sec.67 - Punishment for distributing or transmitting profane material in electronic structure.- Whoever distributes or transmits or causes to be distributed or transmitted in the electronic structure, any material which is lecherous or bids to the obscene intrigue or if its impact is, for example, to will in general debase and degenerate people who are likely, having respect to every significant situation, to peruse, see or hear the issue contained or exemplified in it, will be rebuffed on first conviction with detainment of either depiction for a term which may stretch out to three years and with fine which may reach out to five lakh rupees and in case of a second or resulting conviction with detainment of either portrayal for a term which may stretch out to five years and furthermore with fine which may reach out to ten lakh rupees.

Sec.67A - Punishment for distributing or transmitting of material containing explicitly unequivocal act, in electronic structure and so on. Whoever distributes or transmits or causes to be distributed or transmitted in the electronic structure any material which contains explicitly express act or lead will be rebuffed on first conviction with detainment of either portrayal for a term which may stretch out to five years and with fine which may reach out to ten lakh rupees and in case of second or ensuing conviction with detainment of either depiction for a term which may stretch out to seven years and furthermore with fine which may reach out to ten lakh rupees.

Sec.67B - Punishment for distributing or transmitting of material portraying kids in explicitly unequivocal act, and so on., in electronic structure Abusing kids on the web, detainment for a term which may reach out to five years and with a fine which may stretch out to ten lakh rupees and in case of second or resulting conviction with detainment of either depiction for a term which may stretch out to seven years and furthermore with fine which may reach out to ten lakh rupees.

Sec.67C - Preservation and maintenance of data by delegates: (1) Intermediary will safeguard and hold such data as might be indicated for such span and in such way and arrangement as the Central Government may recommended. (2) Any delegate who deliberately or purposely negates the arrangements of sub-segment (1) will be rebuffed with a detainment for a term which may reach out to three years and will likewise be at risk to fine.

Sec.72 - Penalty for rupture of secrecy and protection: Save as generally gave in this Act or some other law until further notice in power, any individual who, in compatible of any of the forces gave under this Act, standards or guidelines made thereunder, has tied down access to any electronic record, book, register, correspondence, data, report or other material without the assent of the individual concerned uncovers such electronic record, book, register, correspondence, data, archive or other material to some other individual will be rebuffed with detainment for a term which may reach out to two years, or with fine which may stretch out to one lakh rupees, or with both.

Sec. 75 - Act to apply for offenses or negation submitted outside India: (Subject to the arrangements of subsection (2), the arrangements of this Act will apply likewise to any offense or contradiction submitted outside India by any individual regardless of his nationality. (2) For the motivations behind sub-area (1), this Act will apply to an offense or contradiction submitted outside India by any individual if the demonstration or lead establishing the offense or repudiation includes a PC, PC framework or PC system situated in India.

Conclusion

As technology advances, cyberattack methods are evolving as well. Attackers are now more skilled at identifying weaknesses in the system, gathering and analysing vulnerabilities, and locating gaps to obtain access and cause network disruptions. Banks are now implementing the newest cyber-security technology and are willing to pay more money to secure their environment from unauthorised access, unneeded data breaches, and security lapses in order to become well-aware of and advanced with the current hacking techniques. The banking industry can be shielded from unwanted attacks by properly configuring and maintaining firewalls. Banks should use a variety of safety precautions to thwart any such known cyberattacks. A penetration test, which simulates an attacker trying to penetrate the security system, is used to assess the network and infrastructure security of banks on the premises. The goal of the test is to uncover system weaknesses and breaches. Many of these tests have been conducted in the past, and based on the information gathered from those investigations, it was discovered that the majority of vulnerabilities discovered in Indian banks are related to web applications, inadequate network security, ineffective password management, incorrect server configuration, and ignorance.

Conflict of Interest

There is no conflict of interest by the authors in this manuscript.

References

1. Acharya, Suman and Joshi, Sujata (2020). Impact of cyberattacks on banking institutions in India: A study with special of safety mechanisms and preventive measures. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(6), 4656-4670.
2. Jamra, R.K., Anggorojati, B., Sensuse, D.I. and Suryono, R.R. (2020). Systematic Review of Issues and Solutions for Security in E-commerce. In 2020 International Conference on Electrical Engineering and Informatics (ICELTICs), 1-5.
3. Rao, Harshita Singh (2019). Cybercrime in Banking Sector. International Journal of Research Granthaalayah, 7(1), 148-161.
4. Sarangam, Ajay (2020). Cyber Security Challenges in India. Jigsaw Academy. https://www.jigsawacademy.com/cybersecurity-challenges-in-india/.
5. Pawar, Dr. Ashok Shankarrao and Rathod, Dr. Sunita J. (Pawar), Pawar, Dr. Manish Parshuram and Rathod, Niraj J. (2013). Incorporation of Information Technology Act in Banking Transactions. Indian Journal of Applied Research, 3(9), 158-160.